UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----------x

ELENA GELMAN, individually and on behalf of all others similarly situated,

Plaintiff

CLASS ACTION

-against-

NORTHWELL HEALTH, INC. and PERRY JOHNSON & ASSOCIATES, INC.,

DEMAND FOR JURY TRIAL

Defendants

----------x

CLASS ACTION COMPLAINT

Plaintiff, Elena Gelman ("Plaintiff"), brings this Class Action Complaint ("Complaint") against Defendants, Northwell Health, Inc. ("Northwell") and Perry Johnson & Associates, Inc. ("PJA") (collectively "Defendants"), as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions, and upon information and belief and her counsels' investigation as to all other matters, as follows:

INTRODUCTION

1. Plaintiff seeks monetary damages and injunctive and declaratory relief arising from Defendant's failure to safeguard the Personally Identifiable Information[1] ("PII") and Protected Health Information ("PHI") (together, "Private Information") of its patients, which resulted in unauthorized access to its information systems on or around between April 7, 2023 and April 19, 2023 and the compromised and unauthorized disclosure of that Private Information, causing

[1] The Federal Trade Commission ("FTC") defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8). To be clear, according to Defendant, not every type of information included in that definition was compromised in the subject data breach.

widespread injury and damages to Plaintiff and the proposed Class (defined below) members.

2. Defendant, Northwell Health, Inc., is a New York private not-for-profit hospital servicing over 2 million patients each year.[2]

3. Defendant, PJA is a third-party vendor of health information technology solutions used by Northwell.

4. As explained in detail herein, on or around May 2, 2023, PJA detected unusual activity in its computer systems and ultimately determined that an unauthorized third party accessed its network and obtained certain files from its systems between April 7 and April 19, 2023 ("Data Breach").[3]

5. As a result of the Data Breach, which Defendants failed to prevent, the Private Information of Defendants' patients, including Plaintiff and the proposed Class members, were stolen, including their name, date of birth, address, medical record number, hospital account number, and clinical information such as name of the treatment facility, the number of your healthcare providers, admission diagnosis, and date(s) and time(s) of service.[4]

6. Defendants' investigation concluded that the Private Information compromised in the Data Breach included Plaintiff's and over ***three million*** other individuals' information (together, "Patients").[5]

7. Defendants failure to safeguard Patients' highly sensitive Private Information as exposed and unauthorizedly disclosed in the Data Breach violates its common law duty, New York law, and Defendants implied contract with its Patients to safeguard their Private Information.

---

[2] https://www.northwell.edu/about-northwell (last accessed Nov. 10, 2023).
[3] The "Notice Letter." Attached hereto as ***Exhibit A***.
[4] *Id.*
[5] https://longisland.news12.com/northwell-health-vendor-patient-information-may-have-been-impacted-by-data-breach (last accessed Nov. 10, 2023)

8. Plaintiff and Class members now face a lifetime risk of identity theft due to the nature of the information lost, which they cannot change, and which cannot be made private again.

9. Defendants harmful conduct has injured Plaintiff and Class members in multiple ways, including: (i) the lost or diminished value of their Private Information; (ii) costs associated with the prevention, detection, and recovery from identity theft, tax fraud, and other unauthorized use of their data; (iii) lost opportunity costs to mitigate the Data Breach's consequences, including lost time; and (iv) emotional distress associated with the loss of control over their highly sensitive Private Information.

10. Defendants failure to protect Patients' Private Information has harmed and will continue to harm over one million of Defendants' Patients, causing Plaintiff to seek relief on a class wide basis.

11. On behalf of herself and the Class preliminarily defined below, Plaintiff brings causes of action against Defendants for negligence, negligence *per se*, and breach of implied contract, seeking an award of monetary damages and injunctive and declaratory relief, resulting from Defendant's failure to adequately protect their highly sensitive Private Information.

PARTIES

12. Plaintiff is, and at all times mentioned herein was, an individual resident and citizen of the State of New York.

13. Plaintiff obtained healthcare or related services from Northwell. As a condition of receiving services, Northwell required Plaintiff to provide them with her PII/PHI.

14. Based on representations made by Northwell, Plaintiff believed Northwell implemented and maintained reasonable security to protect her PII/PHI.

15. If Plaintiff had known that Defendant would not adequately protect her Private Information, she would not have allowed Defendant to maintain this sensitive Private Information.

16. Defendant Northwell is a corporation organized under the laws of New York with its headquarters and principal place of business at 2000 Marcus Avenue, New Hyde Park, New York 11042.

17. Defendant Perry Johnson & Associates is a Nevada corporation with its principal place of business at 1498 W Warm Springs Rd., Henderson, NV 89014.

JURISDICTION AND VENUE

18. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members is over 100, and at least one Class member is a citizen of a state that is diverse from Defendants' citizenship. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A)

19. This Court has personal jurisdiction over Defendant Northwell Health Inc., because it is a corporation incorporated under the laws of New York, has its principal place of business in New York, and does a significant amount of business in New York.

20. This Court has personal jurisdiction over Defendant Perry Johnson & Associates, Inc., because it transacts business within this state and makes or performs contracts within this state.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Northwell has its principal place of business located in this District, and a substantial part of the events giving rise to this action occurred in this District.

FACTUAL BACKGROUND

Defendant Northwell Health Inc.'s Business

22. Northwell is a New York-headquartered private not-for-profit hospital serving New York City, Long Island and Westchester. As the largest Private Healthcare Provider in New York, Defendant is treats over 2 million patients annually and employs over 79,000 employees.[6]

23. Plaintiff and Class members are current or former Patients who provided their Private Information to Northwell.

24. To obtain medical services, Patients, including Plaintiff and Class members, were required to provide sensitive and confidential Private Information, including their names, dates of birth, health records, insurance information, and other sensitive information, that would be held by Northwell in its computer systems.

25. The information held by Northwell at the time of the Data Breach included the unencrypted Private Information of Plaintiff and Class members.

26. Upon information and belief, Northwell made promises and representations to its Patients that the Private Information collected would be kept safe and confidential, the privacy of that information would be maintained, and Northwell would delete any sensitive information after it was no longer required to maintain it.

27. Indeed, Northwell's own Privacy Practices disclosure provides:

> At Northwell Health, we not only care for your well-being, we are also committed to protecting the security and privacy of your personal health information. We utilize sophisticated technologies and processes to protect your data, and we require that our external partners and vendors meet the same high standards we follow.[7]

[6] https://www.northwell.edu/sites/northwell.edu/files/2022-04/we-are-northwell-fact-sheet-april-2022.pdf (last accessed Nov. 10, 2023)
[7] https://www.northwell.edu/about-northwell/commitment-to-excellence/protecting-patient-privacy (last accessed Nov. 10, 2023)

28. Plaintiff and Class members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

29. Plaintiff and Class members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiff and Class members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

30. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class members from involuntary disclosure to third parties. Defendant has a legal duty to keep Patients' Private Information safe and confidential.

31. Defendant had obligations under the FTC Act, HIPAA, contract, industry standards, and representations made to Plaintiff and Class members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

32. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class members' Private Information. Without the required submission of Private Information, Defendant could not perform the services it provides.

33. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class members' Private Information from disclosure.

Defendant Perry Johnson & Associates, Inc.'s Business

34. PJA "provides medical transcription services to various healthcare organizations."[8] Northwell used PJA for medical transcription and dictation services.[9]

35. Plaintiff and Class members are current or former patients of Northwell and entrusted Northwell with their PII/PHI.

The Data Breach

36. On or about November 3, 2023, Defendants began notifying Patients of the Data Breach, informing them by Notice of Data Breach ("Notice")[10]:

> PJ&A serves as a vendor to Northwell Health, Inc., and its subsidiaries and affiliates (collectively "Northwell"). PJ&A provides certain transcription and dictation services to Northwell. In order to perform these services, PJ&A receives personal health information regarding Northwell patients.
>
> **What Happened?**
>
> PJ&A became aware of a data security incident impacting our systems on May 2, 2023. We immediately initiated an investigation and engaged a cybersecurity vendor to further provide support in connection with our investigation and secure against potential system vulnerabilities. We promptly implemented the cybersecurity vendor-recommended actions to prevent the further disclosure of data as we continued to investigate the situation. Through our investigation, we determined that the unauthorized access to our systems occurred between March 27, 2023 and May 2, 2023, and the unauthorized access to Northwell patient data specifically occurred between April 7, 2023 and April 19, 2023.
>
> On July 21, 2023, PJ&A notified Northwell that an unauthorized party had accessed and downloaded certain files from our systems. PJ&A has preliminarily determined

---

[8] *Cyber Incident Notice*, PERRY JOHNSON & ASSOCS., https://www.pjats.com/downloads/Notice.pdf (last accessed Nov. 10, 2023)

[9] *See* Kevin Vesey, *Cyberattack Targets Northwell Health Vendor; Patient Data Compromised*, NEWS12 (Nov. 9, 2023 6:52 PM), https://longisland.news12.com/northwell-health-vendor-patient-information-may- have-been-impacted-by-data-breach.

[10] Notice Letter

that Northwell data was impacted on May 22, 2023 and, by September 28, 2023, confirmed the scope of the Northwell data impacted.

What Information Was Involved?

We have confirmed that certain files containing your personal health information were impacted by this incident. Specifically, the following information may have been impacted: your name, date of birth, address, medical record number, hospital account number, and clinical information such as name of the treatment facility, the number of your healthcare providers, admission diagnosis, and date(s) and time(s) of service.

What We Are Doing?

We are committed to maintaining the privacy and security of your information and take this incident very seriously. PJ&A took, and will continue to take, appropriate steps to address this incident, including updating our systems to prevent incidents of this nature from occurring in the future. As soon as we learned of the unauthorized access to our systems, PJ&A immediately initiated and investigation and retained a cybersecurity vendor to assist with containing the threat and with further securing our systems. PJ&A notifies law enforcement about the incident and continues to cooperate with law enforcement's investigation.

37. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class members, such as encrypting the information or deleting it when it is no longer needed, causing the exposure of Private Information.

38. The attacker accessed and acquired files in Defendants' computer systems containing unencrypted Private Information of Plaintiff and Class members, including their names, addresses, phone numbers, dates of birth, health insurance information, medical record numbers, patient account numbers, dates of service and/or treatment information. Plaintiff's and Class members' Private Information was accessed and stolen in the Data Breach.

39. Plaintiff further believes her Private Information, and that of Class members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

The Defendants Acquire, Collect, and Store Plaintiff's and Class Members' Private Information.

40. As a condition to obtain medical services from Northwell, Plaintiff and Class members were required to give their sensitive and confidential Private Information to Northwell.

41. Northwell retains and stores this information and derives a substantial economic benefit from the Private Information that it collects. But for the collection of Plaintiff's and Class members' Private Information, Northwell would be unable to perform its services.

42. By obtaining, collecting, and storing the Private Information of Plaintiff and Class members, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting the Private Information from disclosure.

43. Plaintiff and Class members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendants to keep their Private Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

44. Defendants could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiff and Class members.

45. Upon information and belief, Defendants made promises to Plaintiff and Class members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information.

46. Defendants' negligence in safeguarding the Private Information of Plaintiff and Class members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

Defendants Knew or Should Have Known of the Risk of a Cyber Attack Because Healthcare Entities in Possession of Private Information Are Particularly Suspectable to Cyber Attacks.

47. Data thieves regularly target entities in the healthcare industry like Defendants due to the highly sensitive information that they maintain. Defendants knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

48. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting healthcare entities like Defendants that collect and store Private Information and other sensitive information, preceding the date of the Data Breach.

49. In light of recent high profile data breaches at other industry-leading companies, including, *e.g.*, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the Private Information that it collected and maintained would be targeted by cybercriminals.

50. For example, of the 1,862 recorded data breaches in 2021, 330 of them, or 17.7%, were in the medical or healthcare industry.[11]

[11] 2021 Data Breach Annual Report (ITRC, Jan. 2022), https://notified.idtheftcenter.org/s/, at 6.

51. The 330 breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[12]

52. Entities in custody of PHI and/or medical information reported the largest number of data breaches among all measured sectors in 2022, with the highest rate of exposure per breach.[13] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that victims were often forced to pay out of pocket costs for healthcare they did not receive in order to restore coverage.[14] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. 40 percent of the patients were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals, and detrimentally impact the economy as a whole.[15]

53. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the Private Information of Plaintiff and Class members from being compromised.

54. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' server(s), amounting to over one million individuals'

---

[12] *Id*.
[13] *See* Identity Theft Resource Center, *2022 Annual Data Breach Report*, https://www.idtheftcenter.org/publication/2022-data-breach-report/ (last accessed Nov. 10, 2023).
[14] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed Nov 10, 2023).
[15] *See id.*

detailed Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

55. The injuries to Plaintiff and Class members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class members.

56. The ramifications of Defendants' failure to keep secure the Private Information of Plaintiff and Class members are long lasting and severe. Once Private Information is stolen fraudulent use of that information and damage to victims may continue for years.

57. As a healthcare entity in possession of its Patients' Private Information, Defendants knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiff and Class members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class members because of a breach. Nevertheless, Defendants failed to take adequate cybersecurity measures to prevent the Data Breach.

Defendants Fail to Comply with FTC Guidelines

58. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

59. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer

networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[16]

60. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[17]

61. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

62. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

63. These FTC enforcement actions include actions against healthcare entities, like Defendants. *See, e.g.*, *In the Matter of LabMD, Inc., a corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's

[16] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Nov. 10, 2023).
[17] *Id.*

data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

64. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

65. Defendants failed to properly implement basic data security practices.

66. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Patients' Private Information or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

67. Upon information and belief, Defendants were at all times fully aware of its obligation to protect the Private Information of its Patients; Defendants was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendants' conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

Defendants Fail to Comply with HIPAA Guidelines.

68. Defendants are covered businesses under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"),

and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

69. Defendants are subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[18] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

70. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

71. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

72. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

73. "Electronic protected health information" is "individually identifiable health information . . . that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

74. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

[18] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

d. Ensure compliance by its workforce.

75. HIPAA also requires Defendants to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendants are required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

76. HIPAA and HITECH also obligate Defendants to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic PHI that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

77. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

78. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of PHI in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

79. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed

guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[19] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.[20]

Defendants Owed Plaintiff and Class Members a Duty to Safeguard their Private Information.

80. In addition to its obligations under federal and state laws, Defendants owed a duty to Plaintiff and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Plaintiff and Class members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class members.

81. Defendants owed a duty to Plaintiff and Class members to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees and others who accessed Private Information within its computer systems on how to adequately protect Private Information.

[19] https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last accessed Nov. 10, 2023)
[20] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (last accessed Nov 10, 2023).

82. Defendants owed a duty to Plaintiff and Class members to implement processes that would detect a compromise of Private Information in a timely manner.

83. Defendants owed a duty to Plaintiff and Class members to act upon data security warnings and alerts in a timely fashion.

84. Defendants owed a duty to Plaintiff and Class members to disclose in a timely and accurate manner when and how the Data Breach occurred.

85. Defendants owed a duty of care to Plaintiff and Class members because they were foreseeable and probable victims of any inadequate data security practices.

The Data Breach Increases Plaintiff's and Class Members' Risk of Identity Theft.

86. The unencrypted Private Information of Plaintiff and Class members will end up (if it has not already ended up) for sale on the dark web, as that is the *modus operandi* of hackers.

87. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class members.

88. Simply put, unauthorized individuals can easily access the Private Information of Plaintiff and Class members because of the Data Breach.

89. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

90. Plaintiff's and Class members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used

in a variety of sordid ways for criminals to exploit Plaintiff and Class members and to profit from their misfortune.

Loss of Time to Mitigate the Risk of Identity Theft and Fraud

91. As a result of the recognized risk of identity theft, when a data breach occurs and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm.

92. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class members must monitor their financial accounts for many years to mitigate the risk of identity theft.

93. Plaintiff and Class members have spent, and will spend additional time in the future, on a variety of prudent actions, such as changing passwords and resecuring their own computer systems.

94. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[21]

95. Plaintiff's mitigation efforts are also consistent with the steps the FTC recommends data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering an extended

[21] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf (last accessed Nov. 10, 2023).

fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[22]

96. And for those Class members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

Diminution of Value of Private Information.

97. Private Information is valuable property.[23] Its value is axiomatic, considering the value of Big Data in corporate America and that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates, beyond doubt, that Private Information has considerable market value.

98. The Private Information stolen in the Data Breach is significantly more valuable than the loss of, say, credit card information in a large retailer data breach. Victims affected by those retailer breaches could avoid much of the potential future harm by simply cancelling credit or debit cards and obtaining replacements. The information stolen in the Data Breach is difficult, if not impossible, to change.

99. This kind of data, as one would expect, demands a much higher price on the dark web. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black

[22] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last accessed Nov 10, 2023).
[23] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," at 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last accessed Nov. 10, 2023) ("GAO Report").

market."[24]

100. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[25]

101. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[26] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[27,28] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[29]

102. As a result of the Data Breach, Plaintiff's and Class members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class members for their property, resulting in an

[24] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hackpersonal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Nov. 10, 2023).
[25] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private Information") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).
[26] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last accessed Nov. 10, 2023).
[27] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last accessed Nov. 10, 2023).
[28] https://datacoup.com/ (last accessed Nov. 10, 2023).
[29] https://www.thepennyhoarder.com/make-money/nielsen-panel/#:~:text=Sign%20up%20to%20join%20the,software%20installed%20on%20your%20computer (last accessed Nov. 10, 2023).

economic loss. Moreover, the Private Information is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

103. The fraudulent activity resulting from the Data Breach may not come to light for years.

104. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class members are incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

105. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' network, amounting to millions of individuals' detailed Private Information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

106. The injuries to Plaintiff and Class members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class members.

The Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary.

107. Given the type of targeted attack in this case, the sophisticated criminal activity, the volume of data compromised in this Data Breach, and the sensitive type of Private Information involved in this Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

108. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Private Information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

109. Consequently, Plaintiff and Class members are at an increased risk of fraud and identity theft for many years into the future.

110. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class member. This is a reasonable and necessary cost to monitor and protect Class members from the risk of identity theft resulting from Defendants' Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class members would not need to bear, but for Defendant's failure to safeguard their Private Information.

Loss of the Benefit of the Bargain

111. Furthermore, Defendants poor data security deprived Plaintiff and Class members of the benefit of their bargain. When agreeing to pay Defendants for the provision of its services, Plaintiff and other reasonable consumers understood and expected that they were, in part, paying for the service and necessary data security to protect the Private Information when, in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendants.

Plaintiff's Experience

112. Plaintiff obtained medical services from Northwell. To obtain these medical services, she was required to provide her Private Information to Northwell.

113. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's Private Information in its system.

114. Plaintiff is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

115. Plaintiff learned of the data breach after reviewing the Notice. According to the Cybersecurity, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties. The Private Information comprised some combination of her name, date of birth, address, medical record number, hospital account number, and clinical information such as name of the treatment facility, the number of your healthcare providers, admission diagnosis, and date(s) and time(s) of service.

116. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including checking her bills and accounts to make sure they were correct. Plaintiff has spent significant time dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

117. As a result of the Data Breach, Plaintiff fears for her personal financial security and uncertainty over what medical information was revealed in the Data Breach. she is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

118. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

119. As a result of the Data Breach, Plaintiff is presently at risk and will continue to be at increased risk of identity theft and fraud for years to come.

120. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

121. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3), on behalf of a class defined as:

> All individuals whose PII and/or PHI was accessed and/or acquired by an unauthorized party in the Data Breach, including all who were sent a notice of the Data Breach.

122. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

123. Plaintiff reserves the right to amend the definition of the Class or add a Class or Subclass if further information and discovery indicate that the definition of the Class should be narrowed, expanded, or otherwise modified.

124. **Numerosity**: The Class members are so numerous that joinder of all members is impracticable, if not completely impossible. Approximately 3 million individuals were affected by the of the Data Breach. The Class is apparently identifiable within Defendants' records, and Defendants intend to identify these individuals (as stated in the Cybersecurity Notice).

125. Common questions of law and fact exist as to all Class members and predominate over any questions affecting solely individual Class members. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, are the following:

a. Whether and to what extent Defendants had a duty to protect the Private Information of Plaintiff and Class members;

b. Whether Defendants had respective duties not to disclose the Private Information of Plaintiff and Class members to unauthorized third parties;

c. Whether Defendants had respective duties not to use the Private Information of Plaintiff and Class members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the Private Information of Plaintiff and Class members;

e. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

f. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

g. Whether Plaintiff and Class members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendants' wrongful conduct; and

h. Whether Plaintiff and Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

126. **Typicality**: Plaintiff's claims are typical of those of the other Class members because Plaintiff, like every other Class member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Classes.

127. This class action is also appropriate for certification because Defendants acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class members uniformly and Plaintiff's challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

128. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of Class members in that she has no disabling conflicts of interest that would be antagonistic to those of the other Class members. Plaintiff seeks no relief that is antagonistic or adverse to Class members and the infringement of the rights and the damages she has suffered are typical of other Class members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

129. **Superiority**: Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that millions of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class members, who could not individually

afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

130. The nature of this action and the nature of laws available to Plaintiff and Class members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

131. Adequate notice can be given to Class members directly using information maintained in Defendants' records.

132. Further, Defendants have acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

a. Whether Defendants owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

b. Whether Defendants' security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

c. Whether Defendants' failure to institute adequate protective security measures amounted to negligence;

d. Whether Defendants' failure to institute adequate protective security measures amounted to breach of an implied contract;

e. Whether Defendants failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to HIPAA and FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

CAUSES OF ACTION

COUNT I
Negligence
(On behalf of Plaintiff and the Nationwide Class against all Defendants)

133. Plaintiff hereby repeats and realleges all preceding paragraphs contained herein.

134. Defendants requires its Patients, including Plaintiff and Class members, to submit non-public Private Information in the ordinary course of providing health plan services.

135. Defendants gathered and stored the Private Information of Plaintiff and Class members as part of its business of soliciting its services to its Patients, which solicitations and services affect commerce.

136. Plaintiff and Class members entrusted Defendants with their Private Information with the understanding that Defendants would safeguard their information.

137. Defendants had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class members could and would suffer if the Private Information were wrongfully disclosed.

138. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and safeguard their computer property—and Class members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

139. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

140. Defendants owed a duty of care to Plaintiff and Class members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

141. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Patients. That special relationship arose because Plaintiff and Class members entrusted Defendants with their confidential Private Information, a necessary part of being Patients of Defendants.

142. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Private Information.

143. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiff or the Class.

144. Defendants breached their duties, thus were negligent, by failing to use reasonable measures to protect Class members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, (a) failing to adopt, implement, and maintain adequate security measures to safeguard Class members' Private Information; (b) failing to adequately monitor the security of their networks and systems; and (c) allowing unauthorized access to Class members' Private Information.

145. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly considering Defendants' inadequate security practices.

146. It was foreseeable that Defendants' failure to use reasonable measures to protect Class members' Private Information would result in injury to Class members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

147. Defendants had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class members could and would suffer if the Private Information were wrongfully disclosed.

148. Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the

inherent risks in collecting and storing the Private Information of Plaintiff and Class members, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendants' systems.

149. It was therefore foreseeable that the failure to adequately safeguard Class members' Private Information would result in one or more types of injuries to Class members.

150. Plaintiff and Class members had no ability to protect their Private Information that was in, and likely remains in, Defendants' possession.

151. Defendants were in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

152. Defendants' duty extended to protecting Plaintiff and Class members from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

153. Defendants have admitted that the Private Information of Plaintiff and Class members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

154. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and Class members, the Private Information of Plaintiff and Class members would not have been compromised.

155. There is a close causal connection between Defendants' failure to implement security measures to protect the Private Information of Plaintiff and Class members and the harm,

or risk of imminent harm, suffered by Plaintiff and Class members. The Private Information of Plaintiff and Class members was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

156. As a direct and proximate result of Defendants' negligence, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of their Private Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

157. As a direct and proximate result of Defendants' negligence, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

158. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

159. Plaintiff and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

160. Plaintiff and Class members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class members.

COUNT II
Negligence *Per Se*
(On behalf of Plaintiff and the Class against all Defendants)

161. Plaintiff hereby repeats and realleges all preceding paragraphs contained herein.

162. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

163. Pursuant to HIPAA, 42 U.S.C. § 1302d *et seq*., Defendants had a duty to implement reasonable safeguards to protect Plaintiff's and Class members' Private Information.

164. Pursuant to HIPAA, Defendants had a duty to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." *See* definition of encryption at 45 C.F.R. § 164.304.

165. Defendants breached their duties to Plaintiff and Class members under the FTC Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

166. Defendants' failure to comply with applicable laws and regulations constitutes negligence *per se.*

167. The injuries to Plaintiff and Class members resulting from the Data Breach were directly and indirectly caused by Defendants' violation of the statutes described herein.

168. Plaintiff and Class members were within the class of persons the Federal Trade Commission Act and HIPAA were intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statues were intended to guard against.

169. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and Class members, Plaintiff and Class members would not have been injured.

170. The injuries and harms suffered by Plaintiff and Class members were the reasonably foreseeable result of Defendants' breach of its duties. Defendants knew or should have known that it was failing to meet its duties and that Defendants' breach would cause Plaintiff and Class members to experience the foreseeable harms associated with the exposure of their Private Information.

171. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class members have suffered injuries and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT III
Breach of Fiduciary Duty
(On behalf of Plaintiff and the Class against Northwell only)

172. Plaintiff hereby repeats and realleges all preceding paragraphs contained herein.

173. This claim is brought by Plaintiff on behalf of all Class members who provided their PII and PHI to Northwell.

174. Plaintiff and the other Class members gave Northwell their PII and PHI believing that Northwell would protect that information. Plaintiff and the other Class members would not have provided Northwell with this information had they known it would not be adequately protected. Northwell's acceptance and storage of Plaintiff's and the other Class members' PII and PHI created a fiduciary relationship between Northwell on the one hand, and Plaintiff and the other Class members, on the other hand, and Plaintiff and the other Class members, on the other hand. In light of this relationship, Northwell must act primarily for the benefit of their patients, which includes safeguarding and protecting Plaintiff's and the other Class members' PII and PHI.

175. Due to the nature of the relationship between Northwell and Plaintiff and the other Class members, Plaintiffs and the other Class members were entirely reliant upon Northwell to ensure that their PII and PHI was adequately protected. Plaintiff and the other Class members had no way of verifying or influencing the nature and extent of Northwell's or their vendors' data security policies and practices, and Northwell were in an exclusive position to guard against the Data Breach.

176. Northwell have a fiduciary duty to act for the benefit of Plaintiff and the other Class members upon matters within the scope of their relationship. They breached that duty by contracting with companies that failed to properly protect the integrity of the systems containing Plaintiff's and the other Class members' PII and PHI, failing to comply with the data security guidelines set forth by HIPPA, and otherwise failing to safeguard Plaintiff's and the other Class members' PII and PHI that they collected.

177. As a direct and proximate result of Northwell's breaches of its fiduciary duties, Plaintiff and the other Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise,

publication, and theft of their PII and PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII and PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII and PHI which remains in Northwell's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII and PHI compromised as a result of the Data breach; (vii) loss of potential value of their PII and PHI; (viii) overpayment for the services that were received without adequate data security.

COUNT IV
Breach of Implied Contract
(On behalf of Plaintiff and the Class against Northwell Only)

178. Plaintiff hereby repeats and realleges all preceding paragraphs contained herein.

179. This claim is brought by Plaintiff on behalf of all Class members who provided their PII and PHI to Northwell.

180. Northwell offered to provide services to its Patients, including Plaintiff and Class members, in exchange for payment.

181. Northwell also required Plaintiff and the Class members to provide their Private Information to receive services.

182. In turn, Northwell impliedly promised to protect Plaintiff's and Class members' Private Information through adequate data security measures.

183. Plaintiff and the Class members accepted Northwell offer by providing Private Information to Northwell in exchange for receiving Northwell services, and then by paying for and receiving the same.

184. Plaintiff and Class members would not have entrusted their Private Information to

Northwell but for the above-described agreement with Northwell.

185. Northwell materially breached its agreement(s) with Plaintiff and Class members by failing to safeguard such Private Information, violating industry standards necessarily incorporated in the agreement.

186. Plaintiff and Class members have performed under the relevant agreements, or such performance was waived by the conduct of Northwell.

187. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose on each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract along with its form.

188. Northwell conduct as alleged herein also violated the implied covenant of good faith and fair dealing inherent in every contract.

189. The losses and damages Plaintiff and Class members sustained as described herein were the direct and proximate result of Northwell's breach of the implied contracts with them, including breach of the implied covenant of good faith and fair dealing.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class members, requests judgment against Defendants and that the Court grants the following:

A. For an order certifying the Class, as defined herein, and appointing Plaintiff and

her Counsel to represent the Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws.

iii. requiring Defendants to delete, destroy, and purge the Private Information of Plaintiff and Class members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class members;

iv. requiring Defendants to implement and maintain a comprehensive information security program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class members;

v. prohibiting Defendants from maintaining the Private Information of Plaintiff and Class members on a cloud-based database;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendants' systems;

x. requiring Defendants to conduct regular database scanning and security checks;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential Private

Information to third parties, as well as the steps affected individuals must take to protect themselves; and

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct an attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment.

D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined by a jury at trial;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury of all issues so triable.

Dated: January 30, 2024.

Respectfully submitted,

By: *Andrew Shamis*
Andrew J. Shamis (NY Bar #5195185)
Leanna A. Loginov (NY Bar #5894753)
SHAMIS & GENTILE, P.A.
14 NE 1st Avenue, Suite 400
Miami, FL 33132
Telephone: 305-479-2299
ashamis@shamisgentile.com
lloginov@shamisgentile.com

Scott Edelsberg *

EDELSBERG LAW, P.A.
20900 NE 30th Ave., Suite 417
Aventura, FL 33180
Telephone: 305-975-3320
scott@edelsberglaw.com

Jeff Ostrow*
KOPELOWITZ OSTROW FERGUSON WEISELBERG GILBERT
1 West Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Telephone: 954-525-4100
ostrow@kolawyers.com

Attorneys for Plaintiff and the Putative Class

**Pro hac vice forthecoming*